Introduction to the course on digital commerce and emerging technologies

UNCTAD e-commerce week 2018

Marilia Maciel
Digital Policy Senior Researcher
MariliaM@diplomacy.edu
• Intermediary liability
• Personal data protection, privacy, and cross-border data transfers.
• The use of cryptographic technologies or algorithms.
• Disclosure of source code
• Data localisation
• How domain name disputes should be resolved.
• Measures to be taken to control spam.
• Network neutrality
• Cyber-espionage.
• Cybersecurity
• Privacy and data protection
• Data localisation
Cybersecurity
Negative effects of cybercrime

- Financial loss
- Diminished consumer trust
- Loss of trade secrets
- Refusal of access to certain markets
- In some cases, there could be threats to critical infrastructure, to financial and banking systems, and to national security.
Cybersecurity: overview

- Type of action
- Tools and methods (ex. Malware, botnets, DDoS, phishing, ransomware, e-scams)
- International policy frameworks and initiatives (international, regional, bilateral, global initiatives, private sector-led)
- Encryption
- Digital signatures
Example WTO

• Feb 2018: US communication (S/C/W/37) in CTS expressing concerns over Chinese Regulation ‘Cleaning up and Regulating the Internet Access Service Market’. Restrictions for cross-border service suppliers.

• Sep 2017: US communication (S/C/W/374) concerns over China’s cybersecurity law.
Example WTO

• Debates in CTS have revolved around topics, such as:
  – How requirements fall more disproportionately on foreign providers.
  – How such measures affect trade in services in sectors where there are GATS commitments, thus potentially resulting in a violation of the National Treatment principle.
Privacy and data protection
Almost impossible to complete a digital commerce transaction without providing private information.

Protecting this information from leaking or being unduly shared with third parties has become increasingly difficult.

In 2014, eBay reported that 145 million customers had their names, addresses, dates of birth, and passwords compromised.
INDIVIDUAL

STATE

NO CHOICE

DATA

BY CHOICE

DATA

TRACKING AND REPORTING
(Main challenge of digital politics)

BUSINESS
Data localisation
Types of data localisation

• Voluntary

• Forced
  – Data servers located in a particular jurisdiction
  – Influence routing patterns
  – Mandatory purchasing or ownership of data storage equipment
Figure 6. The growth of data localisation provisions  
Source: Bauer et al., 2014
Arguments

- National security
- Curb foreign surveillance
- Protection of privacy
- Law enforcement
- Tax information

- Protectionism
- Non-tariff barrier to trade
- Fragmentation of the Internet
- Human rights concerns
Visit:
www.diplomacy.edu
www.diplointernetgovernance.org

Read our just-in-time reports from the UNCTAD e-commerce week:
dig.watch/unctad2018

Contact:
diplo@diplomacy.edu
mariliam@diplomacy.edu

Twitter:
@DiplomacyEdu @GenevaGIP
@mariliam